OASIS Committee Note

Mobile Alerting Practices Version 1.0

Committee Note 01

18 July 2023

This stage:
https://docs.oasis-open.org/emergency/mapcn/v1.0/cn01/mapcn-v1.0-cn01.docx (Authoritative)
https://docs.oasis-open.org/emergency/mapcn/v1.0/cn01/mapcn-v1.0-cn01.html
https://docs.oasis-open.org/emergency/mapcn/v1.0/cn01/mapcn-v1.0-cn01.pdf

Previous stage:
N/A

Latest stage:
https://docs.oasis-open.org/emergency/mapcn/v1.0/mapcn-v1.0.docx (Authoritative)
https://docs.oasis-open.org/emergency/mapcn/v1.0/mapcn-v1.0.html
https://docs.oasis-open.org/emergency/mapcn/v1.0/mapcn-v1.0.pdf

Technical Committee:
OASIS Emergency Management TC

Chair:
Elysa Jones (elysajones@yahoo.com), Individual

Editor:
Mark Wood (mark.wood@DRCF.net), Disaster Relief Communications Foundation

Abstract:

One method of reaching people with emergency alert messages is via their personal mobile devices, such as mobile phones and tablets. Access to these devices is via the Mobile Network to which they are currently attached. However, the need to make a large-scale distribution in a specific geographic area without crashing the control channel, and the need to reach roamers, whose devices may retain their default behavior from their home network, needs consideration by those mobile networks. This document discusses how practitioners have considered this matter.

Status:

This is a Non-Standards Track Work Product. The patent provisions of the OASIS IPR Policy do not apply.

This document was last revised or approved by the OASIS Emergency Management TC on the above date. The level of approval is also listed above. Check the "Latest stage" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency#technical

TC members should send comments on this document to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/emergency/

Citation format:

When referencing this document, the following citation format should be used:

[Mobile-Alerting-v1.0]

Mobile Alerting Practices Version 1.0. Edited by Mark Wood. 18 July 2023. OASIS Committee Note 01. https://docs.oasis-open.org/emergency/mapcn/v1.0/cn01/mapcn-v1.0-cn01.html. Latest stage: https://docs.oasis-open.org/emergency/mapcn/v1.0/mapcn-v1.0.html.

Notices:

Table of Contents

1 Introduction

1.1 Changes from earlier Versions

This is the first version of this document.

1.2 Glossary

1.2.1 Definitions of terms

1.2.2 Acronyms and abbreviations

1.2.3 Document conventions

- Naming conventions
- Font colors and styles
- Typographical conventions

1.3 Section Title

2 Mobile Alerting.

2.1 What is Mobile Alerting?

Alerting the Public via their personal devices has the advantage of reaching the population in a direct personal way, reaching 90% of them within about 7 seconds or so, using a device normally literally on their person or in arms reach from them. The person buys this device at their own expense, charges it up every night and promptly repairs any faults at their own expense. Visitors to the country also bring their own personal devices with them, but to ensure that they work, some work on standardization is needed.

But the only way to reach such devices is via the mobile network to which they are currently attached, which depends on the location that they are currently in. Very complex Mobility Management Technology is needed to facilitate this, but it does enable the user to roam freely all over the world with their device. In this document, this fact is what defines a Mobile Network as opposed to the fixed network or wireless fixed network, and accordingly Defines 'Mobile' Alerting Practices.

2.2 Technology.

Mobile service is provided by 'Cells', small areas of radio signal cover, which are typically about (1 - 3Km) from the mobile phone user. This is because mobile phones have low power transmitters, poor antennas and are often inside buildings.

The problem faced by a mobile system designer is not what you might think. In fact, the biggest headache is interference from his own base stations and users. So, the antennas are designed to beam their signal down, like a spotlight, not straight out all around like a lighthouse. As the demand for radio frequencies is much greater than the allocation from the government, designers are forced to re-use the frequencies very closely, hence another reason for the small cells. But this can work to our advantage.

Each logical Cell may be supported by several Radio Transceivers, which in turn are connected to a system of antennas, designed to point to the physical geographical area where they are supposed to provide service. This is called the 'Sector'.

The sector antennas are mounted on a tower or the wall of a building. The Radio Transceivers are often in a cabinet or in a room within a few meters of the antennas. This is called the 'Site'. Overland connections back to the Mobile Switching center are provided from the site, either by a land line connection or a microwave relay link system.

The 'Cell' is providing connectivity in the sector to which the antennas are pointing, but it also has hundreds of different logical parameters which can select which mobile devices should use that specific cell, depending on such things as frequency band and system technology (e.g., 2G, 3G, 4G, 5G.). Individual circuits to each transceiver supporting each cell, then fan out to the Radio Base Stations from the MSC.

It is not possible to access an individual Cells directly at the location of the Radio Base Station (e.g., the tower) because cells are linked back to their serving MSC. So, circuits must be routed logically to the serving Mobile Switching Centre, MSC, which may be hundreds of KM away.

There are no people at the Radio Base Station site, Mobile Networks are administered from the Network Operations Centre (NOC), where operations technicians reside. Normally the NOC and MSC are co-sited in the same office as the administrative headquarters of the company, but this is not always so.

For example, in small island states in the Caribbean area, sometimes only the Radio Base Stations are situated on the island, but the Cells are connected to an MSC which is sited at the headquarters of the service provider, which may be off the territory but still firmly under the regulatory oversight of that territory. Regardless of the actual physicality of how the components are physically situated, we can consider the technology to be logically a tree with the only entry point at the MSC.

Though ring and mesh configurations are sometimes used on the backhaul to the radio base stations, to provide redundancy, each logical cell is being administered separately from the MSC.

2.2.1 Short Message Service (SMS).

SMS is administered by a unit called the “SMS Gateway”; a server located normally at the NOC. This in turn handles signaling to the HLR, VLR and MSC via internal cabling inside the building. Each separate message to each individual user must be signaled separately.

The advantage is that the server can know which messages have been received by each user, and which cell they were in when they received the message. This information may be useful to rescuers as they can know how many users were in each cell and who they were.

The disadvantage is that SMS is not natively a geo specific method, so a method must be done to find the phone number of each individual user inside the polygon before this process can start. This involves the creation of a database of user locations, with the attendant regulatory requirements.

Also, the resulting large surge of signaling load may be a factor if the network is already in a high state of load. This process may take hours or some time, and messages may be delivered out of order, the so called ‘cascade’ effect.

2.2.2 Cell Broadcast (CB).

CB can get through even if all lines are busy.

Cell Broadcast is administered by a server called the “Cell Broadcast Centre” (CBC).

CB uses a completely different method to transmit messages. Mobiles are being addressed without their number or address, so the sender instead specifies a ‘Polygon’, a geographical free hand shape defined as a series of latitude and longitude World Geodetic System 1984, WGS84 points, in which, when the last point is the same as the first, this defines a ‘Polygon’ of physical geographic location to which the message is to be sent.

Alternatively, a Geocode, a given name or number such as a county or a state can define the area to be targeted. For example, in the USA a National Weather Service ‘Specific Area Message Encoding’ (SAME) six-digit numerical number with pre-defined physical polygon borders.

Cell Broadcast is not a new feature of the Mobile Networks, but rather was designed by the same team at the same time as the SMS service was defined in the early ‘90s. It is defined by the 3GPP committee as standard 3GPP 023.041. It was designed to complement the SMS service and so uses complementary technology to achieve delivery of short messages.

Rather than use the ‘Traffic Logical Domain’ of the Cell, it uses the ‘Control Logical Domain’ of the Cell. To do this it needs direct connection to a server called the Base Station Controller (BSC), Radio Network Controller (RNC) or directly to the gNodeB which is responsible for administration and maintenance of the cell’s resources, rather than the Mobile Switching Center, MSC, which handles traffic control for customer phone calls and data sessions.

The reason for doing this is because Cell Broadcast uses each cell’s control channel to “Broadcast” the message to all devices listening to the cell, rather than addressing each device individually, one at a time. Therefore, Cell Broadcast can reach limitless millions of devices with a message, even when the system is fully busy, and do so without itself making any more load on the already strained network.

This both makes message delivery more reliable and prevents inadvertently crashing the network with a tsunami wave of signaling load. However, as it does not ‘handshake’ with each user one at a time, there is no record of who has received the message nor any identity of any users inside the polygon.

The CBC takes this polygon and “reverse-engineers” it into a list of ‘Cells’ which provide coverage inside this polygon. Each different CBC vendor has a slightly different method of doing this, but in any case, the translation is not perfect and so some bleeding over of the message outside or inside the polygon often occurs.

However, in WEA version 3, in a useful additional feature called “Device Based Geo-Fencing (DBGF) **ATIS 07 000 41**” the polygon itself may be transmitted, so that a device can determine within a meter or so if it is inside the polygon or not. If not, then it will ignore the message. This give very close adherence to jurisdiction and is very useful for complex territories.

Therefore, to send a Cell Broadcast message, the message, complete with its polygon, must be signaled to the CBC which supports the area under the polygon for each specific network.

In some cases, each network owns and operates its own CBC, which provides access to that networks MSCs.

In other cases, the government owns and operates the common ‘National’ CBC, and each network uses this CBC.

In yet another configuration, a shared CBC is provided by a third-party service provider and is shared by several unrelated networks. This provides low cost of entry to small countries which would otherwise find the cost of such technology prohibitive.

In any case, from a logical point of view, a network can only be accessed via the CBC which is supporting the MSCs providing service to that specific territory. The choice of CBC vendor is normally that of the network unless the government has provided a national CBC.

In fact, the same territory may be being served by several CBCs, one for each participating network. It is unlikely that there will be more than a small handful of CBCs covering a whole territory. For example, the whole of the USA is served by only 15 CBCs.

As this discovery is not automatic, connectivity needs to be engineered into the filtered alert hub systems upstream of the CBC. Normally, the CBC does not carry out any regulatory filtering, this is done further upstream of the CBC at the filtered alert hub or gateway.

2.3 National Sovereignty and Jurisdiction.

Humans do not manage Disasters, they manage Territory.

Broadly, most of the inhabitable land, and some areas of seabed, are a ‘Country’; A set region of land having human occupation or agreed limits, especially inhabited by members of the same race, language speakers etc.

Such countries are administered by Governments; the body with the power to make and/or enforce laws to control a Country.

Government exercises national ‘Sovereignty’ over a territory and defines the society of humans there via a framework of laws and regulations set by that Government. However territorial borders may be disputed, and Governments may change over time, resulting in a change in territorial limits or regulatory environment.

As the Government of that territory has the power to enforce laws and thus control the country, any activity withing that territory may be regulated exclusively by that Government.

Thus, there are no supernational international organizations which have powers superseding the Government of that territory.

Therefore, authority to alert and inform the public, or to give instructions to the population of a territory, is the exclusive right of the Government and is not superseded by any international organization regardless of how well meaning. Ignoring such matters will result in a diplomatic incident and very vigorous enforcement by law enforcement agencies of the Government, fines, prison sentences and lots of litigation liability.

So, of paramount importance is that of national sovereignty and local territorial jurisdiction. So, in the CAP protocol there is a very advanced and secure system, which authenticates prospective senders and verifies their authority in the territory specified in the ‘Polygon’ (the physical land area that the message is targeted to).

If a cross border message is envisaged, national sovereignty needs to be respected. The radio base stations across the border from the sender are physically connected to a different MSC and administered by a different mobile network under a different regulatory framework. The network in turn will be connected to a different CBC and Filtered alert hub, which will be following the regulations of the government of that territory.

Parts of the polygon defined by the sender but in a different jurisdiction will be ignored, but the polygon may be signaled to the alert hub supporting that territory so that its national filtration rules can be applied. At the discretion of the authority, the message may be transmitted from cells in the neighboring territory, subject to their regulations.

Sending unauthorized messages could result in protracted litigation from damaged businesses and diplomatic incidents which are never welcome. It's just as important to prevent a well-meaning sender from overstepping his jurisdiction, as it is to uphold the national sovereignty of the neighboring territory.

Hence an elaborate filtered alert hub system is needed to facilitate wide area cross border information, while also upholding national sovereignty.

2.3.1 Spectrum and Regulatory framework.

How the government controls the networks.

Sovereign nation states have a regulatory ministry of the government responsible for the safe and orderly administration of telecommunications networks in their country, and very importantly, the regulation of the radio spectrum to avoid unintended interference with other radio services. The way this is done differs from one country to the next, but there are also international agreements convened by (but not enforced by) the UN ITU-R secretariat in Geneva.

The radio spectrum is a limited and surprisingly rare resource. The UN ITU-R meets every 4 years to negotiate the sharing of spectrum among 'User Services' and has defined parts of the radio spectrum that can be used for land mobile purposes (such as mobile phones). But it is not very much and needs very careful administration. Currently, in 2023, the scramble for more spectrum for 5G Mobile networks is very vigorous.

However, the word of the national spectrum regulator in each territory will be final.

Enforcement of these regulations is done by a ministry or agency of the government concerned, controlling the leasing of a 'License' to operate the network, and a License to lease radio spectrum for a period (you can lease spectrum, but you can't own it).

A prospective network operator bids for the license on a periodic basis, such as 4 or 8 years, and pays a recurring fee to the government for the issuance of the license. Sometimes the license demands uneconomical 'Universal Service' coverage of the territory, and sometimes it is more 'free market'.

In any case it is an offence to operate a radio network without a license under penalty of very strict enforcement by the national enforcement agency. In addition, the cost of the license may be a considerable fraction of the total cost of operating the network, sometimes up to Billions of dollars!

2.3.2 Alert Authority.

Who can legally say what, where when and how?

The matter of who may give alerts or mandatory instructions to the public is in the purview only of the sovereign Government of the national state. It is not lawful for anyone without authority to give mandatory instructions to a population.

Furthermore, it could be very dangerous both to give uniformed information based on social media rumors and suffer protracted punitive litigation from harmed parties if the sender had no legal cover to do so.

Consequently, a well-defined framework of who can say what, where when and how defines who should safely give such advice or instructions to a population.

Defining such frameworks is the exclusive right of the sovereign national government of the territory. International bodies or commercial corporations do not inherit such rights.

2.3.3 Gateways and Filtered Alert Hubs.

National middleware.

So, there is a further system which is the 'gateway' or 'filtered Alert Hub', to enforce the National and Jurisdictional authority for each authorized sender of an alert message, which can 'Administer the admission of' submitted messages to be sure that they meet with national or regional regulations.

For example, the USA IPAWS OPEN gateway is not merely an aggregator, but also a enforcer of policy regarding USA alerting regulations.

This both prevents embarrassing diplomatic incidents and builds confidence in the public that the messages they see are from properly authorized professionals and not just rumors via social media.

Many Nations have such a system of their own, hosted within their own borders, but there are also proposed shared platforms for such functions under active development at the time of writing, (July 2023).

Though the physical implementation of such filtered hubs may be shared, the logical behavior of the system is still very rigidly upholding the national sovereignty of the territory and enforcing regulations determined by the government of that specific territory.

Due to the urgency of the alert in the acute phase of an emergency, it is valuable if the process is expedited and takes no more than a few seconds.

2.3.4 User Equipment (UE) and special needs for Cell Broadcast.

The phones, smartphones, tablets etc. that the user has.

The terminal will ignore any messages bearing a Message Identifier code (MI) which is not on its list and not work at all if the CB feature is switched off in the phone.

User Equipment, or terminal devices, are such as mobile phones, smart phones, tablets, laptop computers and built-in mobile data modems for Internet of Things (IoT) applications, among others.

One of the advantages of using SMS methods is that no special changes to the UE are needed, however the identity of the device needs to be first discovered in a separate process.

But Cell Broadcast has special needs regarding terminal behavior. Cell Broadcast, as its name suggests, is an entirely passive messaging method, with no signaling occurring between the terminal and the cell.

This does give the advantage of indefinite scalability, immunity from overload of the signaling system and perfect privacy, but it does need special behavior from the terminal for cell broadcast to work.

In some countries, by default the cell broadcast feature is turned off, in some countries it is by default set to intercept only the national alert channels.

A cell Broadcast message begins with a 16-bit binary code, called the Message Identifier (MI). This does not indicate the identity of the receiver or the sender, but rather identifies the kind of information that the following 80 Bytes has. If the device has Cell Broadcast enabled, then it also needs to have a file to tell it which specific Message Identifiers it should intercept.

The terminal will ignore any messages barring a MI which is not on its list, or in a range in the list.

There is a standard published by the 3GPP, **3GPP TS 023.041**, which contains a table listing the published standards for mapping Mis to use cases. This pattern is followed by some countries but not others, so there is a variation of which Mis are used for alerting and warning.

Note that some MIs are mandatory, (that is the user cannot disable them), while others are discretionary, that is the user may disable them manually if he wishes to. The mandatory channels could be used for matters of state security while the other may be used for matters of public safety.

In order to use Cell Broadcast, the terminals in the territory need to have Cell Broadcast enabled and need to have the MI codes for that country opened in the firmware of the phone.

This is done by a well-known ‘over the air activation’ service method or operating system upgrade and is often done successfully on many brands of terminal.

Good news, there is no problem in transmitting on several MIs at once to reach all roamers from neighboring countries if they have a different MI Code.

2.4 Terminal Behavior.

What happens to the phone when it gets an alert?

In addition, the state often needs to terminal to have a different and very intrusive behavior when an alert message has been received, such as a siren sound or other well-known alert sound. Also, the terminal may be required to provide a very intrusive pop-up text on the user screen, which must be acknowledged by the user.

All of this is managed by operating system changes in the terminal device, and so this needs to be installed and initiated in the device to cause this to occur. Accordingly, the mobile networks and the state may consult with terminal vendors in the country to perform this process by over the air methods.

The state may mandate that such features should be enabled by default at the point of sale.

The precise way that this is done is a choice of the state.

In one case, the USA specifies this in document **ATIS 0700036**, which is also used as the basis for some other states in the interest of compatibility for people who are in a territory but from another territory. These are called ‘Roamers’.

2.4.1 Roamers.

Folks who are not from round here.

‘Roamers’ are users who are presently attached to a network which is not their home network. For example, the user may be traveling to another country.

Roaming then becomes a problem. As we know people move around with their own personal mobile device on their person, rather than purchasing a national one when crossing borders. If the phone has been provisioned to open specific MIs, then it will keep these channels open when moving to another territory. If the new territory is using different MIs, then the roamer will miss any alerts while in that territory.

Therefore, if the state wishes to reach roamers, it could do so by transmitting alert messages on the published MI codes. If they wish their own citizens to be alerted when in another territory, then they can open multiple MI codes so that they can intercept them all.

Furthermore, there are national differences in the special alert tone so that citizens will hear a distinctive sound that they are used to which will get their attention. As these very with country, terminals sold in different countries will produce different alert tones and cadences. As this function happens in the phone, when the roamer goes to a different country his alert tone will still be the same as it was at home. This is probably a good thing as this will get their attention better and not cause confusion over a tone that the user does not recognize.

2.4.2 3GPP standards (formerly the GSM committee).

The Third Generation Partnership Project **3GPP** (formerly the GSM committee) is responsible for the technical specification of the signaling interface between devices on the mobile network. Cell Broadcast is a 3GPP standard, and its thanks to their foresight that we have this facility at all. It was introduced into the standard in the early 90s at the same time as SMS was introduced, and by the same engineers. Their standards are open and available for free from their website.

https://www.3gpp.org/specifications-technologies/specifications-by-series

The most important standards for our purposes are.

- **3GPP TS 23.041** (Technical Realization of Cell Broadcast Service).
- **3GPP TS 29.168** (Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3)
- **3GPP TS 36.413** (Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)
- **3GPP TS 36.33 (**Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification)

2.5 Summary of the ATIS documents relating to the USA WEA system and the Canadian NAS system.

The Alliance for Telecommunications Industry Solutions (ATIS) is a leading technology solutions development organization based in Washington DC, USA. ATIS is accredited by the American national standards institute (ANSI). The organization is the north American organizational partner for the 3rd generation partnership project (3GPP), a founding partner of the oneM2M global initiative, a member of the International Telecommunications Union (ITU) as well as a member of the of the inter-American telecommunications commission. For more information visit www.atis.org .

The following ATIS standards relate to the implementation of the USA Wireless Emergency Alert System (WEA) in the United States of America, plus Canada (with national variations)

Other territories also adopt these standards in whole or in part at their own sovereign discretion.

- **ATIS 07 000 06** - Wireless Emergency Alert (WEA) 3.0 via GSM/UMTS [2G,3G] Cell Broadcast service specification.

Superseded.

- **ATIS 07 000 10** - Wireless Emergency Alert (WEA) 3.0 via EPS [4G,5G] Public Warning System Specification.

This document identifies the general requirements for WEA, the specific requirements for the Cell Broadcast Centre (CBC) and the CMSP gateway. The CBC/MME interface is referenced to the appropriate 3GPP standard, while the CMSP gateway to CBC standard is referenced to the appropriate ATIS standard. After referencing the appropriate 3GPP standards for the protocols for Cell Broadcast in general, it goes on to explain the overlying 'Public Warning System' architecture specific to the EPS [4G] system. An overview of WEA element mapping of CBEM to CMAC elements such as message type, message identifier, serial number, list of tracking area ids warning area list repetition period number of broadcast requested data coding scheme and message contents and associated WHAM indicators (for improved polygon resolution).

- **ATIS 07 000 35** - Mobile Device Behavior (Canada).

This document explains how Canadian mobile devices behave when they have received an alert message. The cadence and tones are different from those of the USA.

- **ATIS 07 000 36** - Mobile Device Behavior (USA)

This document explains how USA mobile devices behave when they have received an alert message. The cadence and tones are different from those of Canada.

- **ATIS 07 000 37** - CMSP Gateway specification (C interface).

The Commercial Mobile Service Provider Gateway (CMSP GW) is the interface between the USA Federal government operated IPAWS-OPEN system and the privately owned commercial mobile networks. The CMSP gateway converts the more generic alert message from the IPAWS-OPEN gateway into protocols more specific to the cell broadcast service of that specific network. It also specifies the commercial mobile alert C interface (CMAC) protocol which is used to signal between the IPAWS-OPEN and the CMSP.

- **ATIS 07 000 41** - Device Based Geo-Fencing

Though Cell Broadcast is natively and passively geo specific, (at least down to the area of service of a single cell, about 1KM), the borders of cells don’t follow political borders. To define a reception area, the polygon of the target area can be transmitted more precisely to the device, and its own on-board location system (such as GPS) can define if it is inside the polygon or not). Accordingly, device-based geo fencing specifies how the additional information is signaled to the device.

- **ATIS 07 000 45** - CMSP/CBC interface (D interface)

While the CMSP gateway is an alert specific piece of equipment, with standards set by ATIS, Cell Broadcast is a general-purpose bearer service which long predates WEA and is defined by the 3GPP as it is part of the mobile network. Accordingly, the WEA messages must be translated into parameters needed by the CBC to specify the Cell Broadcast transmission. In 3GPP parlance, the CMSP gateway is just another instance of Cell Broadcast Entity (CBE) which is out of the scope of 3GPP. But while a network can have only one CBC, that CBC can have several CBEs, some of which may not be related to Alerting at all. Therefore, the D interface translates the Alert into parameters specific to Cell Broadcast transmission as defined by the 3GPP.

- **ATIS 07 000 49** - Practical hints.

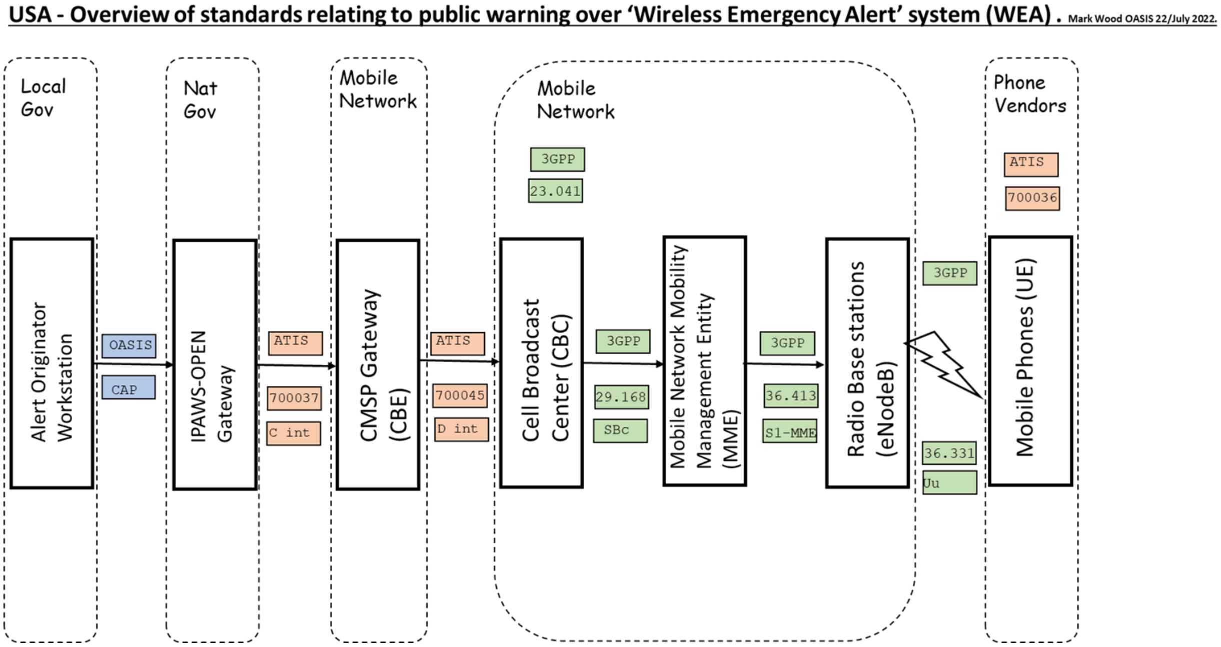
This document is aimed at authorized senders in the USA, with explanations and tips as to how to get the best of WEA. It highlights both the features of the system, and cases where it may be best not to use some features. Matters concerning the selection of geocodes and the decision to use device-based geo fencing are discussed, as well as hints on best practices for the choice of text messages in English and Spanish.

3 National implementation of Mobile Alerting Systems.

NOTE: The order in which the reports are presented is in the order in which contributions to the committee were submitted. No representation of priority or recommendation should be implied by the listing order of the national implementations in this document.

3.1 United States of America. (USA).

Rapporteur. Gary Ham.



USA - Overview of standards relating to public warning over 'Wireless Emergency Alert' system (WEA) . Mark Wood OASIS 22/July 2022.

The United States of American implementation of Wireless Emergency Alert System WEA, (Cell Broadcast implementation).

3.1.1 National Communications Regulators.

In the USA, the Federal Communications Commission (FCC) is the regulator of telecommunications and spectrum licensing in the territory of the USA. It grants licenses to operators of telecommunication networks and radio spectrum users. The FCC grants licenses to the Commercial Mobile Service Providers (CMSP) for the provision of service and the use of spectrum.

3.1.2 Alerting Authorities.

The Federal Emergency Management Agency, (FEMA) by Executive Order 13407, and IPAWS Modernization Act 2015, provides access and administers permissions to the “Wireless Emergency Alert” distribution system (WEA) via the Integrated Public Alert and Warning System, Open Platform for Emergency Networks, (IPAWS-OPEN) gateway system.

The only way to access the WEA system in the USA is via the IPAWS-OPEN gateway. The FEMA IPAWS Project Management Office administers ‘Alerting Permissions’ to ‘Alerting Authorities’ through the administration of IPAWS Project Management Office. A grant to be an IPAWS ‘Alerting Authority’ is granted to, for example, the state and local Alert Agencies, based on permission from the state alerting authority.

Certain Federal agencies have the responsibility to initiate alerts, in which case the IPAWS-OPEN gateway will pass such submissions but under the restrictions specified in that agency’s mission specific responsibilities.

‘Alerting Authorities’ receive their communication authority to access IPAWS-OPEN, from the FEMA IPAWS Project Management Office when they request it and have passed appropriate due diligence. Alerting Authorities can then pass this authority to Alert Originators (People) within their Jurisdiction.

3.1.3 Alert Originators.

‘Alert Originators’ are people who receive ‘Permissions’ granted by their Alerting Authority at State or local level. Responsibility for selecting, training, managing, and authenticating such people, rests with the Alerting Authority.

The administration of the Login ID and the password for individual people is managed locally by the Alert Authority.

3.1.4 Alert Origination software.

‘Alert Origination Software’ is the computer application that the Alert Originators use to input their proposed ‘Alert’ into the IPAWS-OPEN system. It may, for example, reside in a workstation at the office of the ‘Alerting Authority’.

Each ‘Alerting Authority’ is provided an agency specific Identity called the ‘COG ID’ (Collaborative Operations Group Identity), and a digital signature to be used to ‘sign’ the alert and any communications with IPAWS-OPEN. These identities are administered by IPAWS-OPEN office. The Alert Originator Software Vendor includes the ability to configure their software with the COG ID and signature. This permits the Alert Origination application software to access the IPAWS-OPEN Gateway.

The proposed Alert is then converted into a standard Common Alert Protocol (CAP) message, which is then sent using ‘Web Service security’ (WS Security) to the IPAWS-OPEN gateway for authentication.

3.1.5 Distribution Agents (IPAWS-OPEN).

The only way to access the WEA system in the USA is via the IPAWS-OPEN gateway. IPAWS-OPEN gateway authenticates the Alert Originator application software and permits submission of proposed alerts using CAP protocol. The IPAWS OPEN gateway then performs a check on the submission to see that it meets content requirements and permissions authorized. If so, then it is ‘Posted’ as authentic.

One of the ‘content requirements’ is that the ‘Polygon’ (the area to be targeted) consists of no more than 100 “Nodes”. These Nodes are defined by the WGS 84 protocol and defined to 4 decimal points.

Alternatively, a ‘Geocode’ may be used to indicate the area to be targeted, in which case the CMSP gateway ‘reverse engineers’ the polygon or may have a manually defined collection of cells associated with the geocode.

IPAWS-OPEN then converts the ‘Posted Alert’ into the Commercial Mobile Alert for C interface (CMAC) standard and ‘Pushes’ the Alert to Participating Commercial Mobile Service Providers. The Alert is pushed to the ‘CMSP Gateways’ of each participating CMSP, via secure IPSEC/VPN tunnels.

This is called the ‘C’ interface and is governed by the Alliance for Telecommunications Industry Solutions (ATIS) standard ATIS-0700037-. “Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Specification”.

The ‘Gateways’ then internally route Alerts to their Cell Broadcast Centers.

3.1.6 Commercial Mobile Service Providers (CMSP).

Commercial Mobile Service Providers, (CMSPs), are mobile phone network operators, such as

- AT&T,
- Verizon,
- T-Mobile,
- Other national and local service providers in several frequency bands and system technologies.

Wireless Emergency Alert system (WEA) uses Cell Broadcast (CB). This is an existing function of cellular networks defined by the 3GPP (formerly GSM committee) by standard **3GPP 023.041.**

Each participating CMSP hosts its own CMSP gateway or purchases CMSP gateway services from a CMSP gateway host provider. In some cases, the CMSP owns and operates its own Cell Broadcast Centers (CBC), and in some cases the CMSP purchases CBC services from a CBC host provider.

3.1.7 CBC Technology providers.

Here is an example of some of the vendors of this technology, though not exhaustive.

Nokia (Formerly Lucent), Vendor of CBC.

One-to-many (Formerly Logica CMG), Vendor of CBC.

Huawei. Vendor of CBC

Ericsson. Formerly vendor of CBC.

Celtic, CBC vendor.

Velleros, CMSP gateway and CBC providers.

Interop Technologies provides CMSP gateway host services.

3.1.8 User Equipment (UE), Mobile Devices.

User equipment (such as mobile phones) sold in the USA must comply with the standard ***ATIS 0700036.***

While the 3GPP standard **3GPP 023.041** defines the signaling protocols and the message identifiers **MI** to be used for the WEA system, the way that the phone behaves depends on the firmware on board the phone or device and so is vendor specific.

There has been a long-standing gentlemen's agreement that mobile devices must be differentiated in the market as they are a consumer device purchased at the discretion of the end use, so terminal equipment vendors have a lot of latitude as to how the experience is presented to the end user.

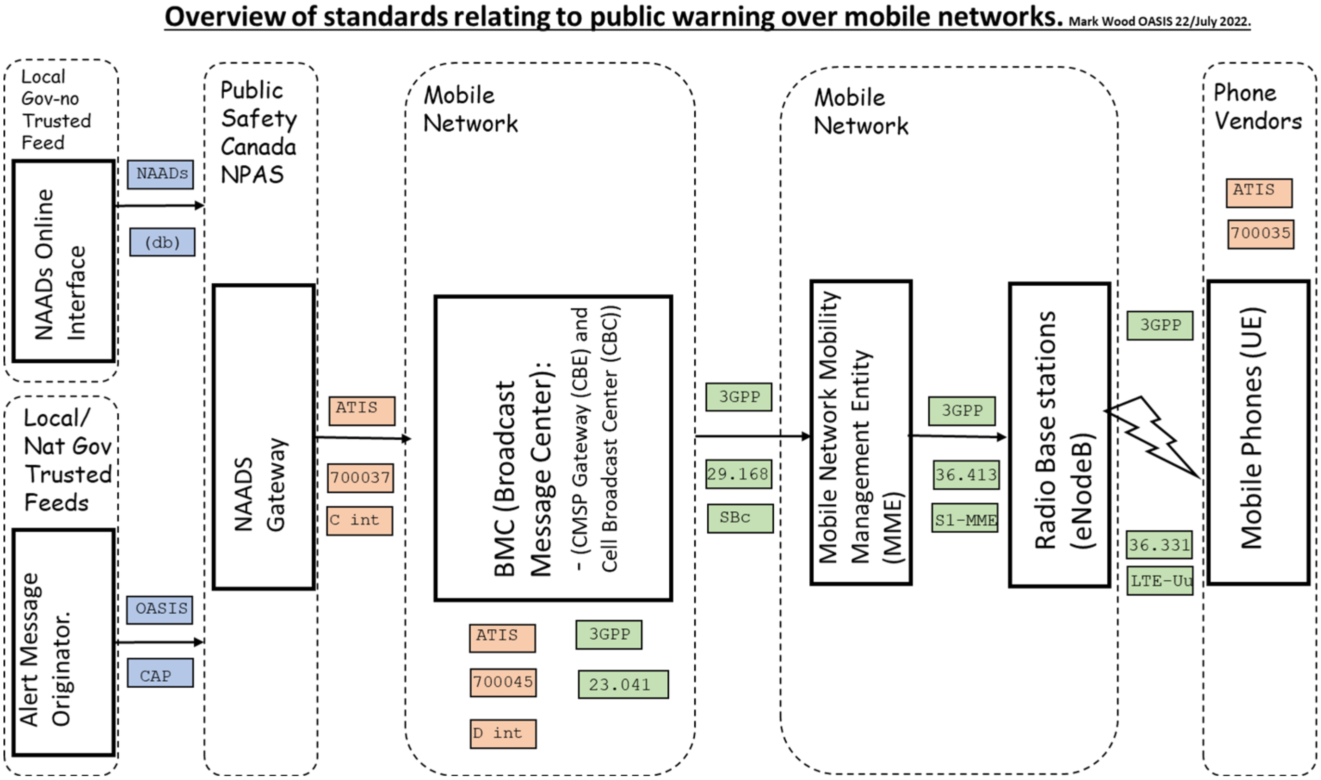
ATIS 0700036**.** Makes requirements of the terminal but does not define how the terminal should achieve the requirement.

3.1.9 Additional Stakeholders.

WIP

3.2 Canada.

Rapporteur. Norm Paulsen.


Overview of standards relating to public warning over mobile networks. Mark Wood OASIS 22/July 2022.
Local Gov-no Trusted Feed
NAADs Online Interface
NAADs
(db)
Local/ Nat Gov Trusted Feeds
Alert Message Originator.
OASIS
CAP
Public Safety Canada NPAS
NAADS Gateway
ATIS
700037
C int
Mobile Network
BMC (Broadcast Message Center): - (CMSP Gateway (CBE) and Cell Broadcast Center (CBC))
ATIS
700045
D int
3GPP
23.041
3GPP
29.168
SBc
Mobile Network
Mobile Network Mobility Management Entity (MME)
3GPP
36.413
S1-MME
Radio Base stations (eNodeB)
3GPP
36.331
LTE-Uu
Phone Vendors
ATIS
700035
Mobile Phones (UE)

The Canadian model for the ‘National Public Alerting System’ (NPAS) , using Cell Broadcast.

3.2.1 National Communications Regulators.

In Canada, the federal department of Innovation, Science and Economic Development Canada is the regulator of telecommunications and spectrum licensing including regulation of the mobile operators. The department is administered by the Minister of Innovation, Science and Industry. Telecommunications legislation: consists of the *Radiocommunication Act*, R.S.C. 1985, c. R-2, *Telecommunications Act*, S.C. 1993, c. 38.

3.2.2 Alerting Authorities.

In Canada, the federal department of Public Safety Canada https://www.publicsafety.gc.ca/index-en.aspx is the custodian of national standards, including standards associated with Public Alerting. The National

Public Alerting System (NPAS) https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ntnl-pblc-lrtng-sstm-en.aspx is a collaborative effort chaired by Public Safety Canada.

Broadcast Distribution Undertakings (BDUs) in Canada operate under national broadcast standards overseen by the Canadian Radio and Telecommunications Commission (CRTC). However, the leadership and oversight for actual Emergency Services and Public Alerting content sits with the 13 Provinces and Territories. Decisions on what and when to Alert the Public vary widely across Canada with some regions receiving a minimal Public Alerting service.

Any Public Alerts calling the population to action technically is under the purview of the Provinces and Territories, and even though federal agencies may issue Public Alerts, there is an understanding that the Provincial and Territorial governments are accepting of this service to a certain point.

Public Safety Canada, however, are the custodians of national standards including the ‘CAP Canadian profile’ (CAP-CP), a subset profile standard of the International CAP messaging standard.

In Canada, the NPAS partners include… Public Safety Canada, who provide oversight to the standards and profiles used by the national system; Pelmorex Inc., a private industry partner who provides the service backbone of the physical operating system; the Canadian Radio and Telecommunications Commission (CRTC), who mandate, upon condition of license, all national and regional BDU’s, of a certain size, to broadcast as content all Emergency Public Alerts, if the alert is defined as an Emergency Public Alert by the authorized agency issuing the alert; and the Provinces and Territories that elect to use the system as part of their Emergency Public Alert strategy.

3.2.3 Others

SOREM (the Senior Officials Responsible for Emergency Management) is the administrative body that is made up of the emergency management organizations representing the 13 Provinces and Territories. Federal representation on this body is included for coordination of national activities and standards. Federal departments may have opinions, but the Provinces and Territories are empowered to create their own appropriate solutions.

Broadly, the Ministry for Emergency Management in each Province and Territory will grant authority for Public Alerting to specific agencies and their agents within their jurisdiction.

3.2.4 Province and Territories:

British Columbia (Emergency Management B.C.)

Alberta (Alberta Emergency Management Agency)

Ontario

Quebec

Newfoundland and Labrador

Etc.

3.2.5 Alert Originator Agencies.

Federal agencies, with jurisdiction on subject matters of national interest (i.e., meteorological, seismological, oceans, international terrorism, etc...), have specific authority for informing the public on events of interest within their domain. Public Alerts are then issued for concerning events within those domains as per the operating mandate of those agencies.

Provincial and Territorial agencies, with jurisdiction on other subject matters of interest (i.e., Health, Emergency Services, Civil matters, Flooding, Forestry, etc.), have similar specific authority for informing the public on concerning events within those domains. Public Alerts are issued within those domains as per the operating mandate of those agencies.

Public Alerts, for subject events that are classified as emergencies, are considered Emergency Public Alerts, and will activate the Alert Ready System in Canada. Emergency Public Alerts can be initiated by all levels of government. However, it is by understanding with the Provinces and Territories that any Call to Action provided be acceptable to the Provinces and Territories. Provinces have the authority to have Public Alerts vetted through their process prior to being released to the Public, but with an understanding, most federal agencies are permitted to alert the public directly.

In Canada, a Public Alert heightens attention about a hazardous or concerning event of interest. Emergency Public Alerts, based on an elevated level of severity of the subject event, and the urgency of the need to be made aware of the event immediately, are warranted to include an additional attention-grabbing mechanism when signaling the public to get the attention of the public more forcibly.

As part of NPAS, wireless cell broadcast Emergency Alerting, and TV and Radio Emergency Alerting, are mandated by the CRTC to occur with any Emergency Public Alert.

For example, Environment and Climate Change Canada may post a blizzard warning that is not considered an Emergency Public Alert, however, the same agency may post a tornado warning that is considered an Emergency Public Alert.

Environment and Climate Change Canada will only mark certain alerts as Emergency Public Alerts based on a pre-determined list of event types, as per SOREM, whether or not a local authority already handles emergency alerting for the event type, as per regional jurisdiction, and their own assessment of the Urgency, Severity and Certainty of the subject event as it compares to the SOREM pre-set list of Urgency, Severity and Certainty settings that qualify as an emergency level.

To facilitate Emergency Public Alerting, SOREM has defined a set of CAP parameter markers in the SOREM CAP Profile that is to direct agents along the path of distribution to establish or modify an intrusive signal with every Emergency Public Alert issued. Last mile software on the receiving end of the path of distribution are to respond to these markers and causing extra audio and visual cues for the intended audiences experiencing the presentation of the alert message.

3.2.6 Alerting Agents.

Alerting ‘Agents’ are individual people designated by Alerting ‘Authorities’ to have the responsibility of issuing alert messages on an as needed basis. Responsibility for selecting, training, managing, and authenticating such agents, rests with the Authority. It is also possible that an automated and approved piece of software could be established and configured to respond to a set of defined environmental conditions causing automated Alert Messages to be generated.

3.2.7 Alerting Software.

Alerting ‘Software’ is the computer application that Alerting Agents use to input their proposed alert into the system.

Any software used to create the resulting CAP Alert Message may be integrated within this software or may be a follow-on piece of software further down the path of distribution. At some point, the proposed alert is converted into a standard Common Alert Protocol (CAP) message, which is subsequently sent via secure tunneling protocol to the National Public Alerting System (NPAS) gateway for processing.

The distribution of Emergency Public Alerts, within the larger NPAS, are then additionally processed in a follow on, but integrated, subset system referred to as the Alert Ready System for immediate and heightened presentation.

The NPAS “National Alert Aggregation & Dissemination System” (NAAD) system hosts a WPAS gateway service architecture, which performs parameter mapping to the “C” interface using WPAC protocol link via secure tunnel to the WSP gateway system pertaining to the participating mobile networks concerned. These then process the signal and send it to the Cell Broadcast Centre (CBC). This in turn selects the cells to be used for the alert and sends commands to each cell over its control channel.

3.2.8 CAP Alerting Agencies.

CAP Alerting ‘Agencies’ are the agencies who have the authority to formalize an Alert message into CAP form and/or send a CAP message across a secure pipe for further distribution. Environment and Climate Change Canada operates in the roles of Alerting Agent, Alerting Authority, and CAP Alerting Agency, whereas the majority of the provinces administer the role of Alerting Agent and Authority but contract out the role of CAP Alerting Agency to Pelmorex Corp.

3.2.9 CAP Alerting Distribution Agents.

CAP Alerting distribution ‘Agents’, facilitate the process of moving the CAP Alert Message down the path of distribution to the Alert’s intended audience. Last Mile distribution ‘Agents’ are then responsible for the presentation of the Alert Message to the intended audience in an acceptable form. All CAP distribution agents along the path of distribution are authorized by either the NPAS system, which in turn is authorized by Public Safety Canada, or the Provinces and Territories for any regional based system should that system involve the CAP standard.

3.2.10 Mobile Network Operators (MNO).

Commercial Mobile Service Providers, (CMSPs), are mobile phone network operators, such as

- Roger’s,
- Bell
- Telus.

3.2.11 Technology providers.

Nokia (Formerly Lucent), Vendor of Broadcast Message controller and CBC.

3.2.12 User Equipment (UE), Mobile Devices.

Canada User Equipment behavior is defined in standard **ATIS 0700035** “Canadian Wireless Public Alerting Service (WPAS) LTE Mobile Device Behavior”. Which is compatible with the USA standard **ATIS 0700036**.

Non-LTE devices are not required to be compatible with WPAS.

The Canadian devices will interpret a Cell Broadcast message as a WPAS alert, if the message identifier value is MI **4370-4399** as per **3GPP TS 023.041**.

Canadian user equipment has a different alert tone than that of the USA. It is the **Canadian Alerting Attention** Signal and the requirement to support French characters by the **UCS-2** standard.

This cadence is 8 seconds long and alternates every 0.5 seconds between Tone1 of 932.33 Hz 1046.5 Hz and 3135.96 Hz modulated at 7271.96 Hz and alternatively with Tone 2 at 440 Hz 659.26 Hz and 3135.96 Hz modulated at 1099.26 Hz.

The Canadian vibration alert cadence is 8 seconds long and is a 0.5 second slow vibration during the sounding of Tone 2.

The Canadian standard also requires that a WPAS alert **Banner** must have the following text “**EMERGENCY ALERT / ALERTE D’URGENCE**.

Canada does not regulate any special pop-up behavior allowing the Network Operators to devise a satisfactory response to an ‘Emergency Public Alert’.

At least one model of user equipment must be available for uses with special needs, such as the blind or the deaf.

3.2.13 Bilingual alerts.

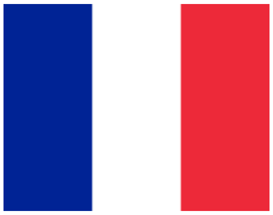
All alerts in Canada must have the capability to be in both official languages in Canada, namely English and French. However regional alerts can be unilingual depending on the region. In any case the **GSM 7-bit character set** cannot transmit all the French characters and so it is mandatory for Canadian devices to be able to support the **UCS-2**-character set.

WPAS alerts may be transmitted as two separate alerts, one for each language. In which case Unilingual people will see from the **Bilingual banner** that there is an alert in progress but should receive the message in their own language a few seconds later.

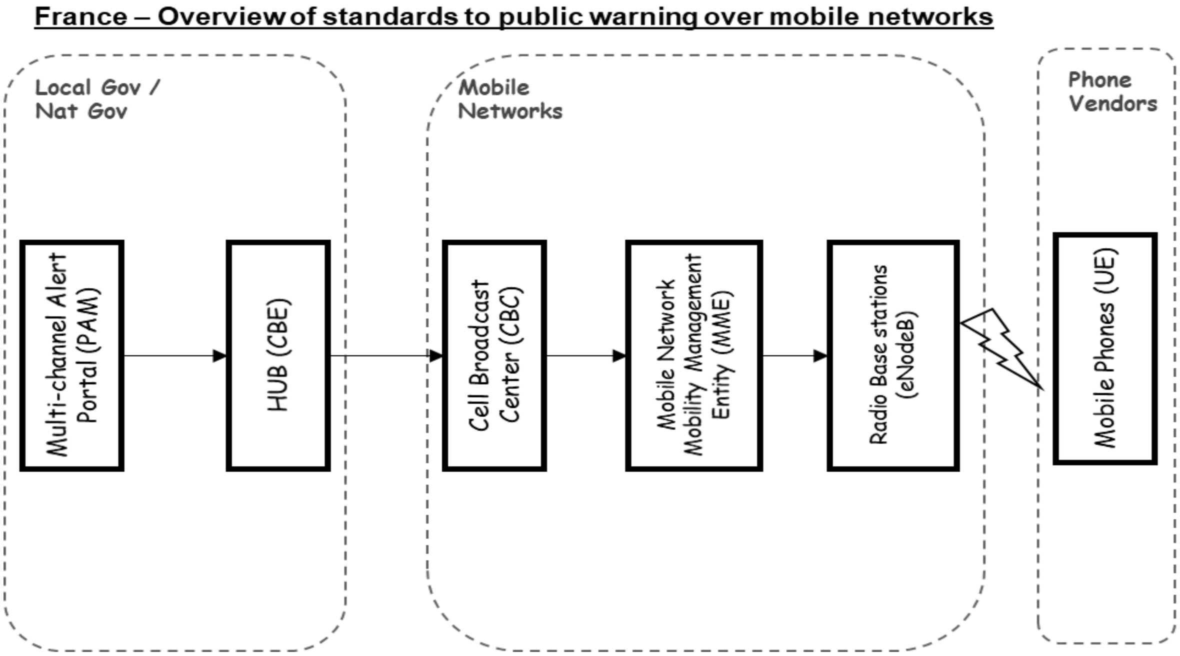
3.2.14 Compatibility with USA

Otherwise WPAS user equipment behavior is largely based on and compatible with the United States WEA system. It therefore complies with **J-STD-100 “Joint ATIS/TIA CMAS Mobile Device Behavior specifications and its supplement A.**

3.3 French Republic, République française



Rapporteur, Patrick Mignotte, French Interior Ministry.


France – Overview of standards to public warning over mobile networks
Local Gov / Nat Gov
Mobile Networks
Phone Vendors
Multi-channel Alert Portal (PAM)
HUB (CBE)
Cell Broadcast Center (CBC)
Mobile Network Mobility Management Entity (MME)
Radio Base stations (eNodeB)
Mobile Phones (UE)

The French PAM system.

3.3.1 National Communications Regulators

In France, the regulator of telecommunications and spectrum licensing in the territory is the Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). It grants licenses to operators of telecommunication networks and radio spectrum users.

3.3.2 Alerting Authorities

The project is led by the Ministry of the Interior. The Digital Directorate of the Ministry of the Interior, as the coordinator of the project, provides access and administers permissions to the PAM (France's multi-channel alert portal).

The decision to alert the population of France is usually taken by authorities linked to the Ministry of the Interior, but it may come from other Ministries depending on their competencies and missions. For example, the Amber alert is decided by authorities under the guidance of the Ministry of Justice. It leads to multiple factor restrictions: geographical, broadcasting channels, event types.

However, alerting competency is mainly led by the Ministry of the Interior. At a national level, the alerting authority is the office of the Minister of the Interior, which oversees French mainland but also French overseas territories. The Ministry of the Interior delegates the alerting competencies to Defense and security Zones (ZDS) led by the Préfet de région that have competencies on multiple Departments, and to Préfectures de département led by the Préfet de département. The authority in charge of the alert will depend on the nature and the scale of the event.

3.3.3 Alerting Agents

'Alerting Agents' are people who receive 'permissions' granted by their Alerting Authority at national or local level. Responsibility for selecting, training, managing, and authenticating such people rests with the Alerting Authority.

Access to the PAM can only be granted to agents who have followed a dedicated training program.

The administration of the user database is managed nationally by the Digital Directorate of the Ministry of the Interior. Local administrators are responsible for updating the list of agents.

3.3.4 Alerting Software

'Alerting Software' is the computer web application that the Alerting Agents use to input their Alert into the PAM. It is only accessible on the Ministry of the Interior Network.

Each 'Alerting Authority' is provided with an agency specific Identity, and a digital signature to be used to 'sign' the alert and any communications with the PAM. These identities are administered by a certification authority under the guidance of the Ministry of the Interior. The Alert Originator Software Vendor includes the ability to configure their software with the signature.

The proposed Alert is then converted into a standard Common Alert Protocol (CAP) message.

3.3.5 Mobile Network Operators (MNOs)

MNOs are mobile phone network operators, such as:

- Orange
- Bouygues Telecom
- SFR
- Free
- Other local service providers in several frequency bands and system technologies on French overseas territories.

The French Wireless Emergency Alert system uses Cell Broadcast (CB) and Location-Based SMS (LB SMS).

In some cases, the MNO owns and operates its own Cell Broadcast Centers (CBC), and in some cases the MNO purchases CBC services from a CBC host provider.

3.3.6 CBC Technology providers

Here is an example of some of the vendors of this technology, though not exhaustive.

Intersec, CBC vendor.

Celtic, CBC vendor.

3.3.7 User equipment (UE), Mobile devices

Mobile operating system providers have implemented specific parameters that have been requested by the French Government regarding the behavior of the smartphone when receiving Cell Broadcasting messages. It mainly concerns the display, ringtone and vibration of the message depending on the Cell Broadcast level.

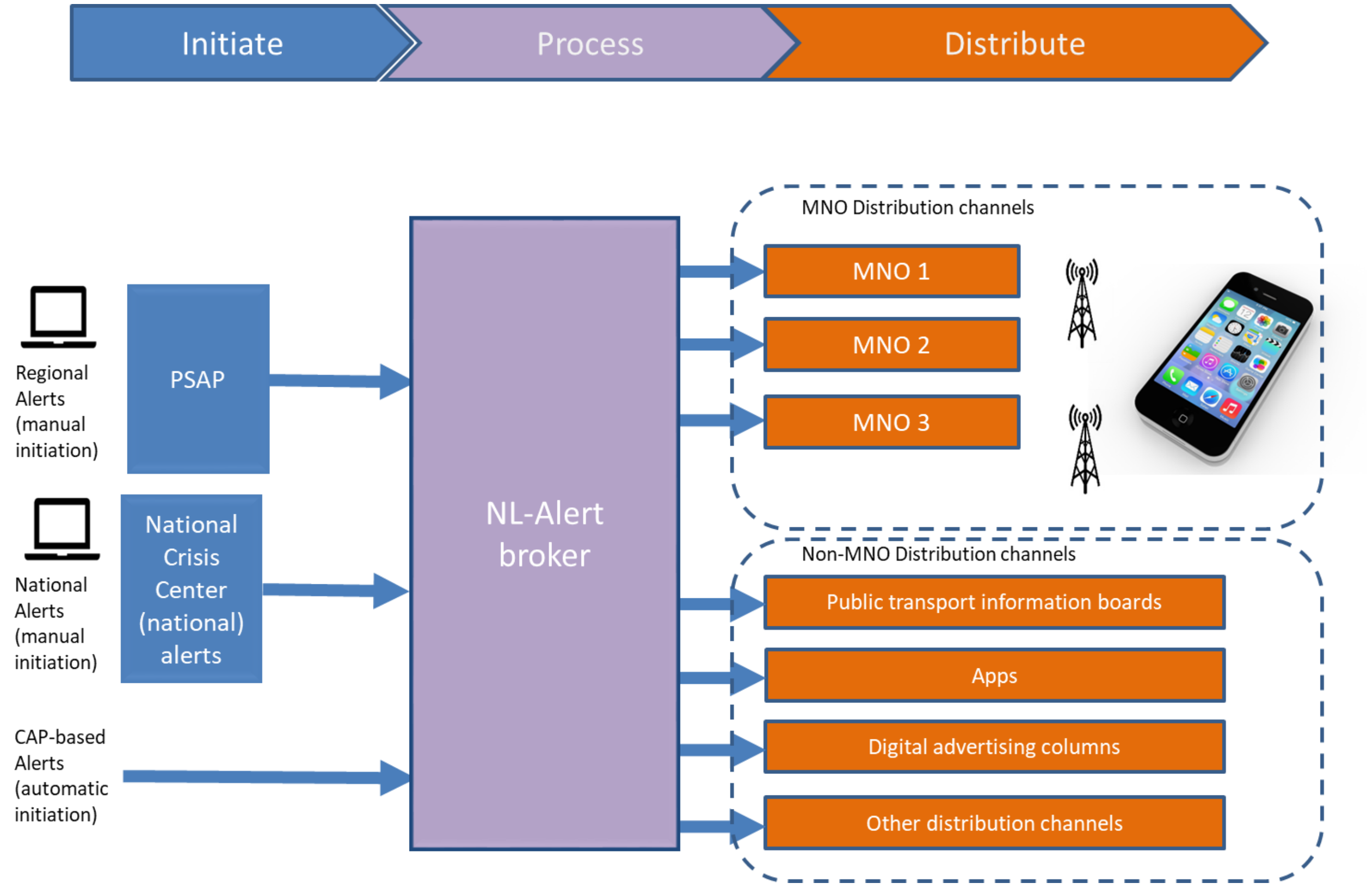
Roamers in coming to France are supposed to reveive french Alerts with those specific parameters.

3.3.8 Additional Stakeholders

The French alert system is called the multi-channel Alert Portal (PAM in French) as it is not specific for the wireless emergency alerts such as CB and LB-SMS. In the future, it will be used for each alert vector: alarm buzzers, social media, variable message panels...

3.4 The Netherlands, Nederland.

Rapporteur, Josine Quist, Ministry of Justice, Netherlands.


Initiate
Process
Distribute
Regional Alerts (manual initiation)
PSAP
National Alerts (manual initiation)
National Crisis Center (national) alerts
CAP-based Alerts (automatic initiation)
NL-Alert broker
MNO Distribution channels
MNO 1
MNO 2
MNO 3
Non-MNO Distribution channels
Public transport information boards
Apps
Digital advertising columns
Other distribution channels

The Netherlands NL-ALERT system.

The Netherlands wireless public alerting system is called **NL-Alert**. This system was launched in 2012 and is now (2023) able to reach around 90% of the population within seconds.

The figure below describes the setup of the NL-Alert system. NL-Alert messages can be initiated manually by (regional) PSAPs of the National Crisis Center. Operators of the system select a distribution area and an alerting message. The alerting message can be selected from a standard library or be free format text. Messages can also be accepted from other (CAP-based) system sources.

The broker is the central system (government gateway) where all system users' login to. The broker **processes** initiated messages and distributes them to the Distribution Channels. The Mobile Network Operators are the main Distribution Channels, but there are also other distribution channels to devices in the public space to enhance the reach of NL-Alert.

3.4.1 National Communications Regulators

In The Netherlands, the regulator of telecommunications and spectrum licensing in the territory is the RDI (Rijksinspectie Digitale Infrastructuur)**.** It grants licenses to operators of telecommunication networks and radio spectrum users.

Please note that the RDI only governs the MNO Distribution Channels and not the rest of the NL-Alert system.

3.4.2 Alerting Authorities

The NL-Alert system is initiated and owned by The Ministry of Justice and Security. The main users are the Security Regions in the Netherlands. Security Regions are responsible for Security in their region, and they get access to the Broker and rights to Distribute NL-Alert messages within the territory of their Region and adjacent Regions. The National Crisis Center also has access to the Broker and has the right to send messages in the whole country.

The responsibility to alert the population in The Netherlands lies with the mayor. All mayors in The Netherlands have mandated this responsibility to the Security Regions since they have a 24/7 operation. So, in practice the Security Regions mostly decide when to alert the population. The guiding principle is that the population is alerted when their life, health or property is in danger.

3.4.3 Alerting Agents

The administration of NL-Alert system users is managed nationally by LMS (Landelijke Meldkamer Samenwerking, National PSAP cooperation), part of the Netherlands Police. They manage the NL-Alert system, provide access rights to users, and give appropriate rights to users of the Broker.

3.4.4 Alerting Software

The Broker contains a webserver with functionality to authenticate users, provide them with rights to use certain functionality of the system, functionality to edit a message and functionality to initiate the distribution-to-Distribution Channels.

3.4.5 Mobile Network Operators (MNOs)

All public MNOs are obliged to support NL-Alert by law. The obligation is to provide a robust Cell Broadcast service via all network infrastructures and technologies (3G, 4G, 5G, etc.) that they provide public services on.

3.4.6 CBC Technology providers.

MNOs are free to select their technology providers.

3.4.7 User equipment (UE), Mobile devices

The Netherlands is using the standard mobile phone behavior features as defined by ATIS.

The Netherlands uses only one cell broadcast channel (**4371**) to make it easy to communicate about NL-Alert with the population.

Since Apple and Google (the main providers of operating systems) nowadays provide more flexibility than ATIS has defined, some local settings may be introduced in the near future.

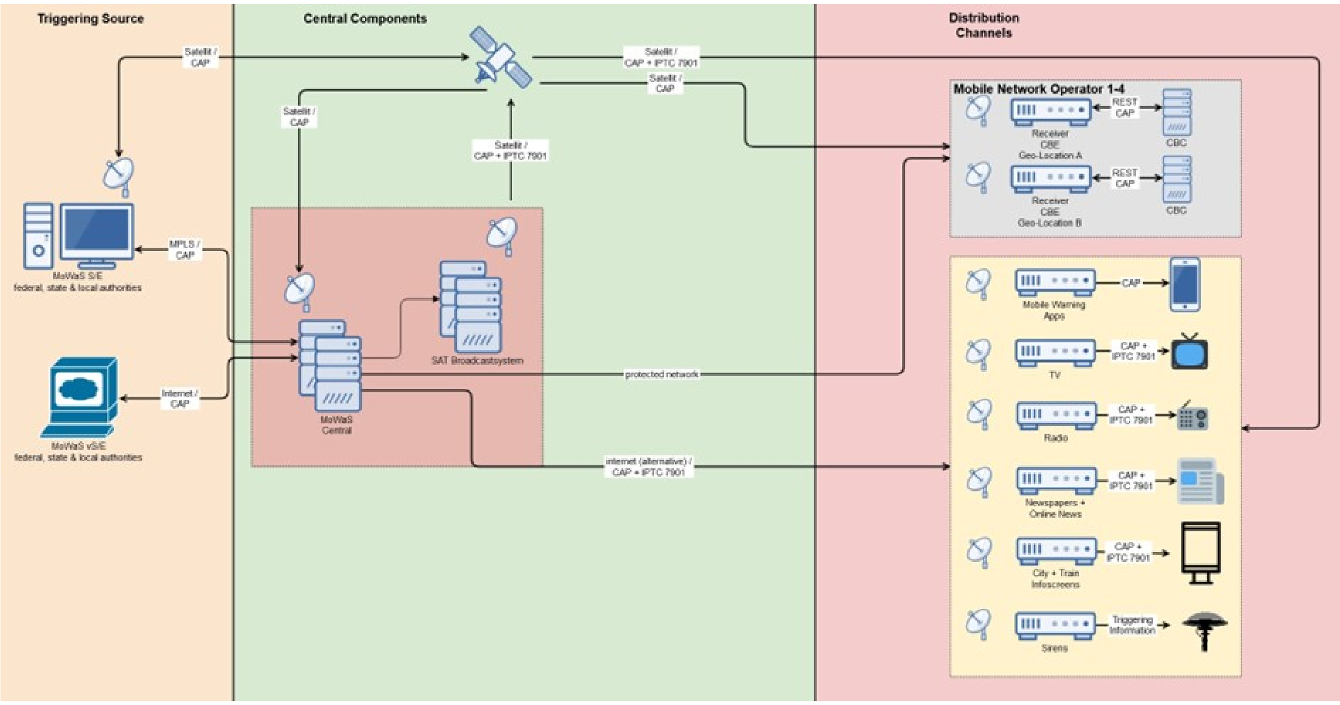
Incoming roamer phones will automatically adopt Netherlands settings and receive NL-Alerts without having to take any further action.

3.4.8 Additional Stakeholders

As mentioned before, The Netherlands has enhanced NL-Alert with many additional Distribution Channels to be able to reach more people that for some reason (i.e., a personal limitation, a specific location, a specific time) are difficult to reach via the MNO/cell broadcast based solution.

3.5 Federal Republic of Germany, Bundesrepublik Deutschland.

Rapporteur, Mandy Best, OASIS CAP committee, mecom.de.



The German modular warning system (MoWaS).

On February 23rd, 2023, Public Warning was introduced via Cell Broadcast in Germany. Using this technology, warnings are broadcasted to mobile devices within a few seconds.

Municipal, state, and federal authorities can trigger warnings via the Modular Warning System (MoWaS). There are two types of MoWaS input systems:

- Hardened transmission- and receiving systems (MoWaS S/E)
- Web-based template-creating transmission- and receiving systems (MoWaS vS/E)

Hundreds of these stations are currently active in Germany, in order to be able to warn the general public of possible events such as fire, severe weather events, harmful emissions, criminal acts of violence, cyber-attacks and many more.

The MoWaS input systems are authenticated via the redundant MoWaS centers.

3.5.1 National Communications Regulators.

In Germany, the Bundesnetzagentur (Federal Network Agency) is the regulatory authority responsible for telecommunications and frequency licenses. This agency issues licenses to telecommunication network operators.

3.5.2 Alerting Authorities.

Various German authorities such as the Federal Office for Civil Protection and Disaster Assistance (BBK), the Federal Ministry of Interior and Homeland Security (BMI), the Federal Office for radiation protection and other are authorized to send warning messages to the entire Federal Republic of Germany.

3.5.3 Alert Originators.

Dispatchers in the control and situation centers of the municipal, state, and federal authorities only ever create warning messages for their area of responsibility.

The BBK is responsible for training and administration as well as granting access and authentication.

3.5.4 Alert Origination software.

The Modular Warning System (MoWaS) is a highly available, geo-redundant and hardened system for warning the population in Germany.

The warning system has three warning levels - low, medium, and high. Based on the warning level and the warning area, the available warning devices are suggested, from which the dispatcher can choose.

Cell broadcast can be used as a warning multiplier at all levels, automatically preselected at the highest level. The dispatcher adds a descriptive text to the warning and sends it.

3.5.5 Distribution Agents.

The warning message is transmitted via a CAP message (Common Alert Protocol), via satellite and terrestrial to the MoWaS headquarters and from there to the selected recipients via satellite and in parallel via the terrestrial route.

In Germany, the technical specifications for cell broadcast are regulated by a technical guideline of the Federal Network Agency (Bundesnetzagentur) as a specification for the MNOs.

A CBE (Cell Broadcast Entity) is installed at each geo-redundant location of a mobile network operator, which receives the CAP messages via satellite and a secure terrestrial path. A cell broadcast-specific CAP message is generated in the downstream system and sent to the CBC of the respective mobile network operator in German and English. Using the geographic coordinates provided in CAP, the MNO controls the corresponding mobile phone tower for transmission.

In order to ensure availability between the CBE and CBC, a keep alive CAP message is sent from the CBE to the CBC at regular short intervals.

3.5.6 Commercial Mobile Service Providers (CMSP).

Commercial mobile network operators in Germany

- Telekom
- Vodafone
- Telefónica
- 1&1

3.5.7 CBC Technology providers.

Following CBC providers are being used:

- Everbridge
- Intersec

3.5.8 User Equipment (UE), Mobile Devices.

Work in progress.

Appendix A Informative References

This appendix contains the references that are used in this document.

While any hyperlinks included in this appendix were valid at the time of publication, OASIS cannot guarantee their long-term validity.

https://www.3gpp.org/specifications-technologies/specifications-by-series

[3GPP TS 23.041]

Technical Realization of Cell Broadcast Service 3GPP TS 23.041.

[3GPP TS 29.168]

Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3 3GPP TS 29.168

[3GPP TS 36.413]

*Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1A) 3*GPP TS 36.413

[3GPP TS 36.33]

Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification) 3GPP TS 36.33

ATIS documents are not open and are available only to members on a fee basis. OASIS does not have permission to publish material from ATIS.

https://www.atis.org/

[ATIS 07 000 35]

Mobile Device Behavior (Canada).

[ATIS 07 000 36]

Mobile Device Behavior (USA)

[ATIS 07 000 37]

CMSP Gateway specification (C interface).

[ATIS 07 000 41]

Device Based Geo-Fencing

[ATIS 07 000 45]

CMSP/CBC interface (D interface)

[ATIS 07 000 49]

Practical hints.

Appendix B Acknowledgments

Appendix B.1 Special Thanks

Thanks to the Editors of this document.

Mark Wood, Disaster Relief Communications Foundation (DRCF) and OASIS CAP committee.
Thomas Wood, Disaster Relief Communications Foundation (DRCF) and OASIS CAP committee.

Special thanks to the National rapporteurs.

Gary Ham, and OASIS CAP committee, (USA Report).
Norm Paulsen, OASIS CAP committee, (Canada Report).
Mandy Best, OASIS CAP committee, mecom.de (Germany Report).

Appendix B.2 Participants

The following individuals were members of this Technical Committee during the creation of this document and their contributions are gratefully acknowledged:

Patrick Mignotte, French interior ministry, (France Report).
Josine Quist, Ministry of Justice, Netherlands (Netherlands Report).

Appendix C Revision History

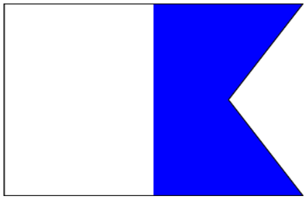
Revision	Date	Editor	Changes Made
1	16/July/2023	Mark Wood	Initial release.

Appendix D Examples of contributions.

Appendix D.1 Single national system example.

Example 1

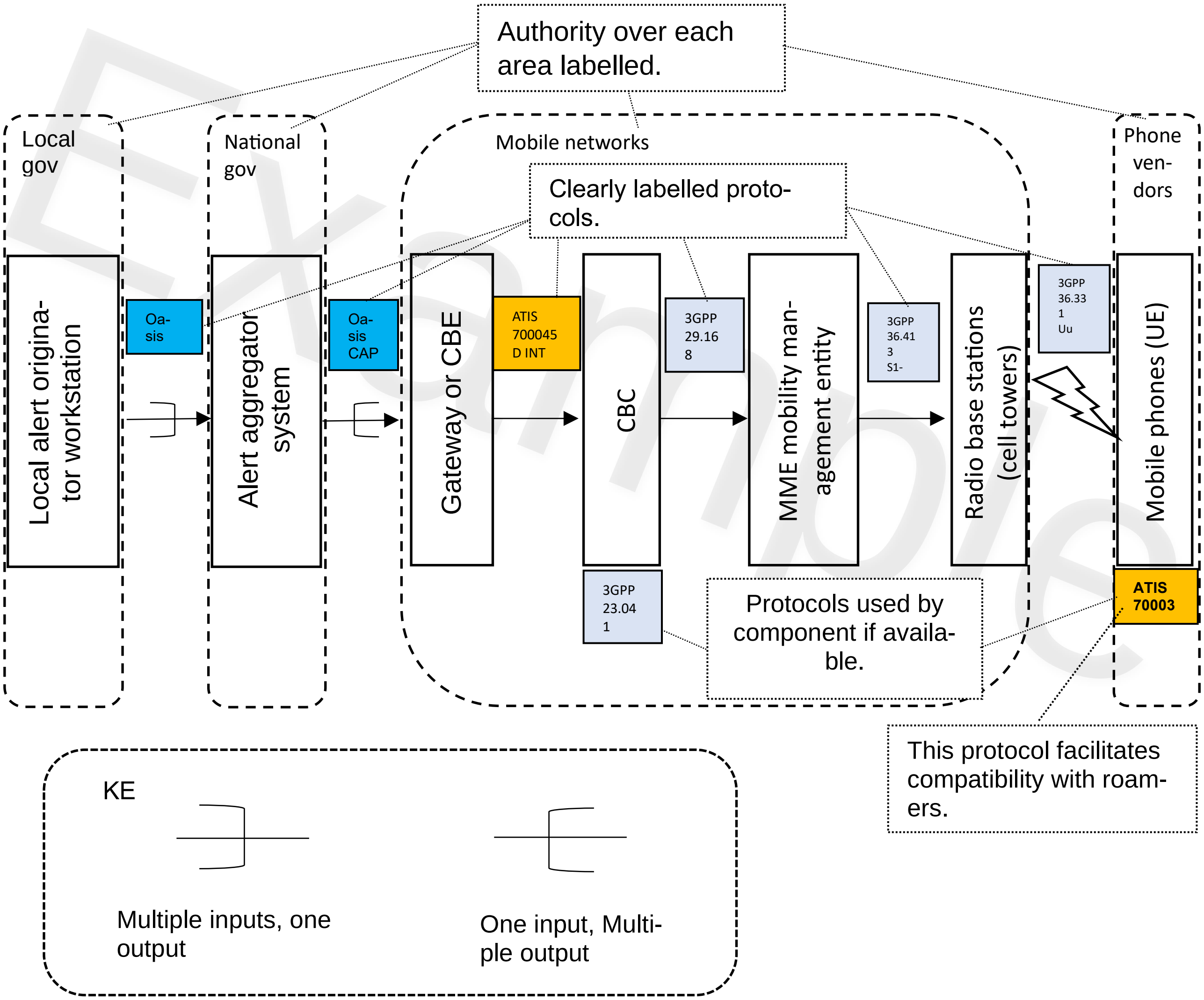
Alpha Land



(Flag or logo)

Rapporteur: Joe Bloggs

contributors name and/or org here. (Optional contact details)

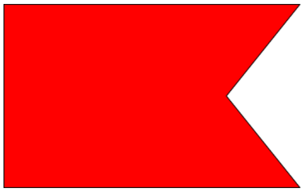


Authority over each area labelled.
Local gov
National gov
Mobile networks
Phone vendors
Clearly labelled protocols.
Local alert originator workstation
Oasis
Alert aggregator system
Oasis CAP
Gateway or CBE
ATIS 700045 D INT
CBC
3GPP 29.168
MME mobility management entity
3GPP 36.413 S1-
Radio base stations (cell towers)
3GPP 36.331 Uu
Mobile phones (UE)
ATIS 70003
3GPP 23.041
Protocols used by component if available.
This protocol facilitates compatibility with roamers.
KE
Multiple inputs, one output
One input, Multiple output
Example

Appendix D.2 Example of a multiple input system.

Example 2 – multiple inputs and specialty software

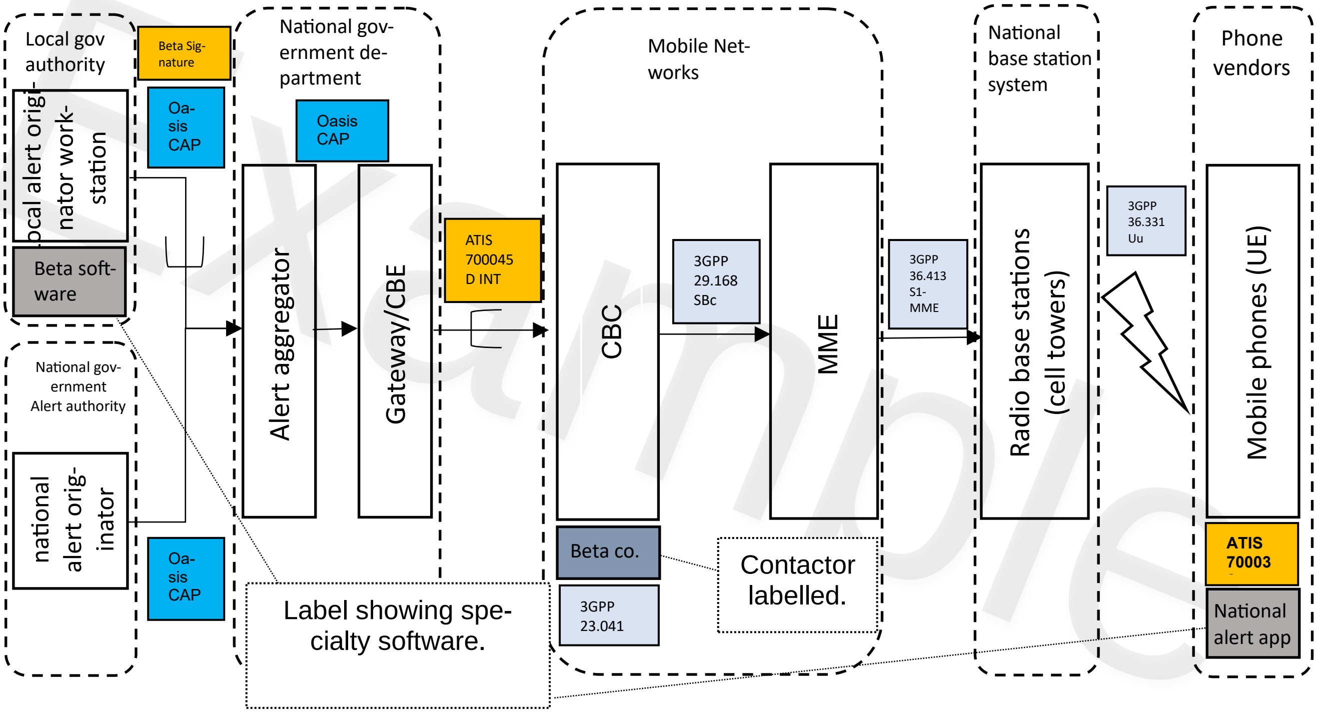
Beta land



(Flag or logo)

Rapporteur: John Doe

contributors name and/or org here. (Optional contact details)



In this example, there are two sperate inputs, one from local government alert authorities with an associated signature that informs the alert aggregator the local AA (alert authorities) permission and denies any overreach from that local station. In addition, a national AA which has the authority to send national scale alerts.

The written section is up to the contributor to decide what to include and explain, in this case it would outline the difference between local AA and national AA and how this is enforced. It would also explain the specialty software and its strengths. And any other aspects that make up system, such as the policy that means all CBC's must be bought from beta co. but are owned by the individual mobile network.

Appendix D.3 Example of shared platforms system.

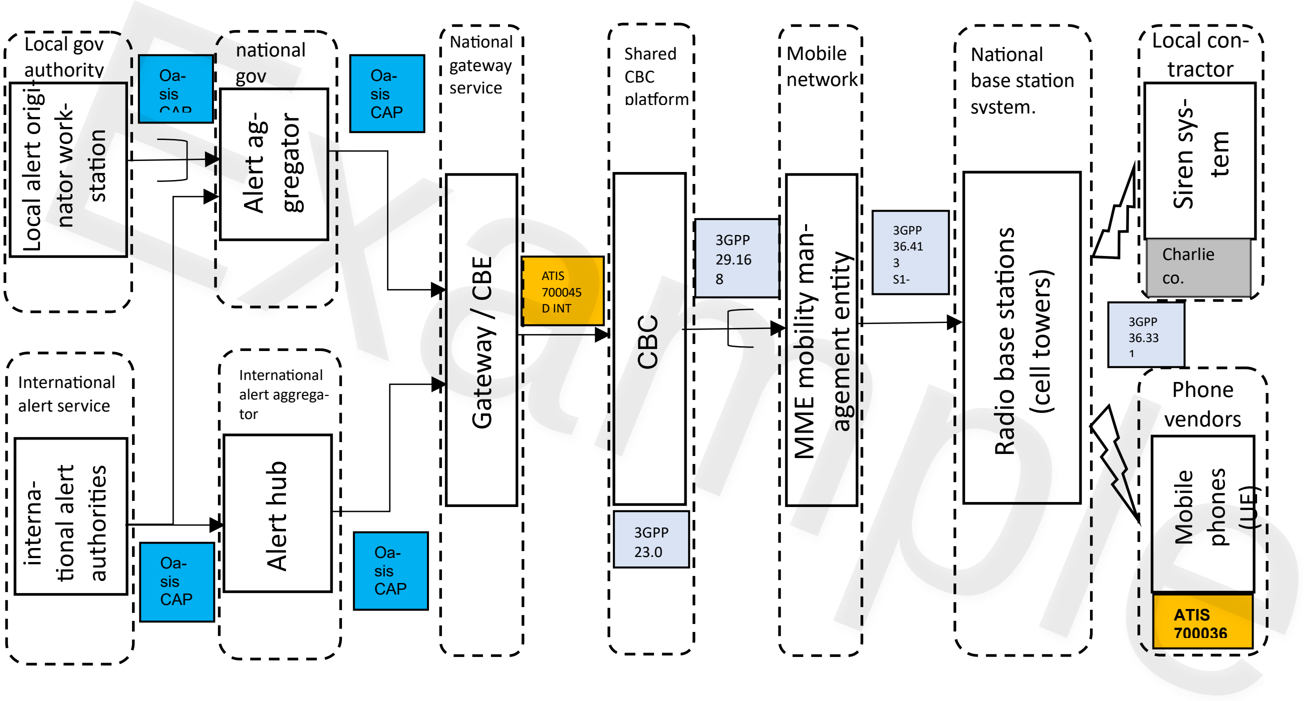
Example 3 – multiple alert aggregators and a shared CBC platform. With a cell broadcast-based siren system

Charlie land

(Flag or logo)

Rapporteur: Tom, Dick, and Harry et al.

contributors name and/or org here. (Optional contact details)



This is an example of a shared CBC's platform. It also has two source inputs for the alert aggregator, one international one local. How cooperation with international organizations is achieved while maintaining the country's sovereignty would be described in the written section.

The shared CBC platform allows smaller scale MNOs to share one CBC between them, in this example only a shared CBC platforms exists but, in some systems, larger MNO's have their own CBC, and others use a shared platform.

Stakeholder in this shared platform would be described in the written section along with any information the contribution deems fit.

<u>Text section of the contribution.</u>

This section can be used as seen fit by the contributor,

It’s recommended to write one paragraph about each component (Each vertical rectangle E.G., local alert origination workstation, alert aggregator system, gateway or CBE, CBC, MME, Radio base stations, mobile phones.)

The policy or regulation that outlines the system should be mentioned, if possible, as it may be necessary to inform the reader on how to proceed with their own project or research.

Appendix E Notices

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OASIS AND ITS MEMBERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THIS DOCUMENT OR ANY PART THEREOF.

The name "OASIS" is a trademark of OASIS, the owner and developer of this document, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, documents, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark/ for above guidance.